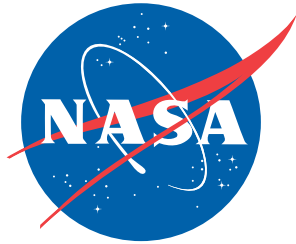


NASA/TM-2012-217558
NESC-RP-12-00762



Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program (CCP)

*Oscar Gonzalez/NESC
Langley Research Center, Hampton, Virginia*

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Report Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

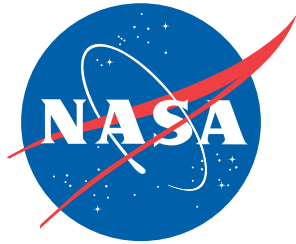
- **TECHNICAL PUBLICATION.** Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.
- **TECHNICAL MEMORANDUM.** Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- **CONTRACTOR REPORT.** Scientific and technical findings by NASA-sponsored contractors and grantees.
- **CONFERENCE PUBLICATION.** Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.
- **SPECIAL PUBLICATION.** Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.
- **TECHNICAL TRANSLATION.** English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, and organizing and publishing research results.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at <http://www.sti.nasa.gov>
- E-mail your question via the Internet to help@sti.nasa.gov
- Fax your question to the NASA STI Help Desk at 443-757-5803
- Phone the NASA STI Help Desk at 443-757-5802
- Write to:
NASA STI Help Desk
NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320

NASA/TM-2012-217558
NESC-RP-12-00762



Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program (CCP)

*Oscar Gonzalez/NESC
Langley Research Center, Hampton, Virginia*

National Aeronautics and
Space Administration


Langley Research Center
Hampton, Virginia 23681-2199

April 2012

The use of trademarks or names of manufacturers in the report is for accurate reporting and does not constitute an official endorsement, either expressed or implied, of such products or manufacturers by the National Aeronautics and Space Administration.


Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320
443-757-5802

| | | | |
|---|---|---|----------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 1 of 43 |

Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program (CCP)

March 15, 2012

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 2 of 43 |

Report Approval and Revision History

| |
|---|
| Approved: _____ <i>Original Signature on File</i> _____ <u>3/26/12</u> <div style="display: flex; justify-content: space-between; width: 100%;"> NESC Director Date </div> |
|---|

| Version | Description of Revision | Office of Primary Responsibility | Effective Date |
|---------|--|--|----------------|
| 1.0 | Initial Release | Mr. Oscar Gonzalez, NASA Technical Fellow for Avionics, GSFC | 3/15/12 |
| 1.1 | Per email 4/3/12 from the JSC Chief Safety Officer (M. Erminger), changed references of Commercial Crew and Cargo Program to Commercial Crew Program. <i>(Director's signature not required)</i> | Mr. Oscar Gonzalez, NASA Technical Fellow for Avionics, GSFC | 4/3/12 |


| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 3 of 43 |


Table of Contents

Technical Assessment Report

| | | |
|-------------|--|-----------|
| 1.0 | Notification and Authorization..... | 5 |
| 2.0 | Signature Page..... | 6 |
| 3.0 | Team List | 7 |
| 4.0 | Executive Summary | 8 |
| 5.0 | It is About Assurance..... | 10 |
| 6.0 | Review of Commercial Crew Provider Rationale for using Commercial Parts | 13 |
| 7.0 | Response to Commercial Crew Program Specific Requests of the NESC | 16 |
| 8.0 | Can COTS EEE Parts Be Used in Flight Hardware Systems?..... | 29 |
| 8.1 | Part of an Established Top-Down Assurance Program..... | 30 |
| 8.2 | Mechanism to Confirm Parts Quality | 31 |
| 8.2.1 | Control the Supply Chain through Qualification and Screening | 31 |
| 8.2.2 | Defend Against Counterfeit Parts | 32 |
| 8.2.3 | Accurate Assessment of Commercial Parts Failure Rates | 33 |
| 8.2.4 | Manage Parts Obsolescence..... | 34 |
| 8.2.5 | Identify Threatening Materials | 34 |
| 8.3 | Establish a Plan to Identify and Recover from a Defective Lot | 35 |
| 9.0 | Conclusions..... | 36 |
| 10.0 | Other Deliverables | 37 |
| 11.0 | Lessons Learned..... | 37 |
| 12.0 | Definition of Terms | 37 |
| 13.0 | Acronyms List | 38 |
| 14.0 | Appendices..... | 39 |

List of Figures


| | | |
|---------------|---|----|
| Figure 5.0-1. | Notional Non-Electrical and Electrical Failure Rate Contributors to Loss of Mission..... | 10 |
| Figure 5.0-2. | Notional Parts Failure Rate and Uncertainty about Median | 12 |
| Figure 7.2-1. | Notional Electronics System Architecture: 3 Cross-Strapped Strings of 24 Boxes..... | 17 |
| Figure 7.2-2. | Failure Probability for a Hypothetical 24-Element, 3-String X-Strap Electronics System versus Parts Grade for 6 Months | 19 |
| Figure 7.2-3. | Failure Probability for a Hypothetical 24-Element, 3-String X-Strap Electronics System Powered Down After 2 Weeks versus Parts Grade..... | 20 |

| | | | |
|---|---|---|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 4 of 43 |

| | | |
|---------------|--|----|
| Figure 7.2-4. | Failure Probability for a Hypothetical 24-Element, 3-String X-Strap Electronics System for a 2-Week Mission versus Parts Grade | 25 |
| Figure 7.2-5. | System Diagram Showing Random and CCFs | 26 |
| Figure 7.2-6. | Failure Probability for a Hypothetical 24-Element 3-String X-Strap Electronics System with CCF of 1 percent for 2nd String and 3 percent for 3rd String versus Parts Grade over a 6-Month Mission..... | 28 |

List of Tables

| | | |
|--------------|--|----|
| Table 5.0-1. | Comparison of Reliability Factors and Parts Grade (adapted from NEPP)..... | 12 |
| Table 7.2-1. | Failure Probability at 6 Months for a Hypothetical 24-Element, 3-String X-Strap Electronics System versus Parts Grade | 19 |
| Table 7.2-2. | Failure Probability for a Hypothetical 3-String X-Strap Electronics System Powered Down After 2 Weeks versus Parts Grade | 20 |
| Table 7.2-3. | General Comparison of MIL versus COTS EEE Parts for High Reliability Applications | 23 |
| Table 7.2-4. | Progression of Failure Probability Considering Mission Length for a Hypothetical 24-Element, 3-String X-Strap Electronics System versus Parts Grade..... | 24 |
| Table 7.2-5. | Failure Probability for a Hypothetical 24-Element 3-String X-Strap Electronics System for a 2-Week Mission versus Parts Grade..... | 25 |
| Table 7.2-6. | Failure Probability for a Hypothetical 3-String X-Strap Electronics System with Various CCF Rates versus Parts Grade over a 6-Month Mission..... | 28 |
| Table 8.0-1. | Assurance Program Elements for Assuring Flightworthy Parts | 29 |

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 5 of 43 |


Technical Assessment Report

1.0 Notification and Authorization

NASA's Commercial Crew Program (CCP) is stimulating efforts within the private sector to develop and demonstrate safe, reliable, and cost-effective space transportation capabilities. One initiative involves investigating the use of commercial electronic parts. NASA's CCP asked the NASA Engineering and Safety Center (NESC) to collect data to help frame the technical, cost, and schedule risk trades associated with electrical, electronic and electromechanical (EEE) parts selection and specifically expressed desire of some of the CCP partners to employ EEE parts of a lower grade than traditionally used in most NASA safety-critical applications.


Dr. Christopher Iannello requested the NESC to investigate this effort. The rationale to support this approach as indicated in the NESC request is discussed in this report along with some considerations and comments by the NESC Avionics Technical Discipline Team (TDT). The out-of-board activity was approved by the NESC Review Board on February 16, 2012.

The key stakeholders for this assessment are the NESC and the CCP.

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 7 of 43 |

3.0 Team List

| Name | Discipline | Organization |
|-------------------------------|---|-----------------------------|
| Core Team | | |
| Oscar Gonzalez | Lead, NASA Technical Fellow for Avionics | GSFC |
| Michael Bay | Avionics TDT/Systems Engineering TDT | Bay Engineering Innovations |
| Mitchell Davis | Avionics TDT/ Chief Avionics System Engineer, Deputy Lead | GSFC |
| Robert Kichak | Electrical Power TDT/Avionics TDT | GSFC-MEI |
| Michael Sampson | AST, Reliability & Quality Assurance | GSFC |
| Consultants/Reviewers | | |
| Yuan Chen | EEE COP | LaRC |
| Lloyd Keith | NESC Chief Engineer | JPL |
| Denney Keys | NASA Technical Fellow for Electrical Power | GSFC |
| Nans Kunz | NESC Chief Engineer | ARC |
| Tim Wilson | NESC Deputy Director | LaRC |
| Administrative Support | | |
| Tricia Johnson | MTSO Program Analyst, NESC | LaRC |
| Erin Moran | Technical Writer | LaRC-ATK |

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 8 of 43 |

4.0 Executive Summary

NASA's Commercial Crew Program (CCP) is stimulating efforts within the private sector to develop and demonstrate safe, reliable, and cost-effective space transportation capabilities. One initiative involves investigating the use of commercial electronic parts. NASA's CCP asked the NASA Engineering and Safety Center (NESC) to collect data to help frame the technical, cost, and schedule risk trades associated with electrical, electronic and electromechanical (EEE) parts selection and specifically expressed desire of some of the CCP partners to employ EEE parts of a lower grade than traditionally used in most NASA safety-critical applications. The original request to the NESC is provided in Appendix A.


The NASA Avionics Technical Fellow and members of the Technical Discipline Team (TDT) responded with comments to the CCP provider's stated rationale for use of commercial parts (refer to Section 6). The NESC team also responded to the specific analytical support requests (refer to Section 7).

The fundamental question posed is *can commercial off-the-shelf EEE parts with limited screening be used in crewed flight hardware systems?*

The term "commercial off-the-shelf parts," or "COTS," is broadly defined and not applied consistently. The medical, automotive, aviation, and some consumer electronics manufacturers are termed commercial users. However, these industries frequently employ supply chain controls to assure the quality and reliability of the EEE parts used in their products. At the other end of the spectrum are commercial catalog parts that have not been subjected to any testing other than functionality.

The NESC team reviewed and analyzed approaches based on screening parts only through box- or system-level testing and concluded that there are fundamental concerns with the rationale (Section 6). The approach is based on procuring commercial parts as received from a distributor without qualification for space or additional screening, and assembling them on circuit boards. Such an approach would result in assembling good parts along with any weak parts, parts with latent defects, and infant mortals into flight hardware with the assumption that board-, box-, and system-level testing can effectively identify parts that might fail during the anticipated mission lifetime.

The team concluded that board-, box-, and system-level testing cannot replicate accelerating factors that voltage, current, and temperature stresses provide during part-level screening (Section 6.0.1). The traditional approach of eliminating non-conforming parts through screening, prior to board installation, has consistently proven effective. Established screening approaches applied at some point along the supply chain identifies defects and abnormalities that are not intended features of the device design, and serve as warning signs of premature failure, reduced performance and safety. Once a part failure occurs, effective two-way traceability of

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 9 of 43 |

commercial parts is necessary to identify the origin of the failed part and location of other similar defective parts within the system.

Qualification is essential to assure the part technology, design, and construction is capable of predictable and required performance in the space environment. Qualification can expose parts that function properly in terrestrial applications but may not perform safely in the more extreme space radiation, vacuum, vibration, and thermal environments.


NASA has successfully used commercial parts in spacecraft for specific and sometimes mission critical applications throughout the Agency's history. This has been achieved by careful selection, qualification, and screening. The level of screening required of commercial parts to assure they will work successfully is highly dependent on the mission, their application, and part technology and is quite well characterized in existing NASA parts documents such as EEE-INST-002. NASA flies non-MIL parts when the required functionality and or performance is not available in MIL parts. If a MIL part can be used, they are preferred.

The NESC team responded to specific questions asked by the CCP Program. Initial qualitative analysis by the NESC team indicates significant differences in reliability and safety can result between screened MIL parts and unscreened commercial parts (Section 7). Differences are highly influenced by mission duration, system architecture, including the selection of like or diverse backup systems.

Automotive, commercial aviation, medical, and safety conscious consumer electronics industries engage in assurance processes within their supply chain to identify weak parts, parts with latent defects, and infant mortals before assembling them into critical applications. The NESC team found no data from any industry or agency supporting delivery of safety critical systems with unscreened parts procured from distributors.

The team concluded that any alternative approach for the use of COTS EEE parts in critical applications other than those which have proved successful, such as described in EEE-INST-002 or similar NASA documents, requires a firm basis for substantiation (Section 7). Any approach, which is based on architectural similar redundancy and box-level testing, has been studied by the NESC team and shown to not be sufficient to enable widespread use of unscreened parts acquired from distributors in critical applications.

To reduce the likelihood that parts failures result in unacceptable mission risk, the NESC recommends the CCP require vehicle providers to: 1) develop and implement a top-down mission assurance program to address EEE parts derating, qualification, traceability, and counterfeit control, and demonstrate how it mitigates the risks associated with EEE parts applications, and 2) provide data supporting the effectiveness of the proposed screening approach assuring part failure rates are adequately bounded. Section 8 of this paper provides insight into some of the major characteristics of a parts assurance program.

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 10 of 43 |

5.0 It is About Assurance

Ultimately, selection of an electronics parts and supply chain management program is driven by assurance principles. Assuring the parts perform as intended and as expected is critical not only to complete mission objectives but, most importantly, for human-rated missions, returning the crew safely to Earth.

There is no *a priori* prescription for low-risk electronics. Even a Grade 1 Class “S” parts program can be defeated by improper parts application and stress issues rooted in design or unforeseen vibration and thermal environmental interactions with parts assembled on the board.

A sound assurance program for low-risk electronics is grounded in a careful top-down assessment of mission risk drivers. Top-down systems engineering identifies and attacks the highest risk (weakest links) whether induced by EEE parts or non-electrical items such as weak risers or attach bolts for the parachute. An assurance program “assures” the actual hardware is designed with margin and is built and performs as intended.

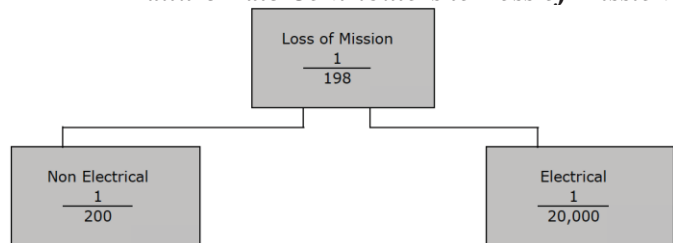
The duration of critical functions can vary widely from a single 2-hour-long use to multiple reuse capsules with 6 months or longer on orbit stay times, which has a major influence on risk.

EEE parts assurance starts with the mission and the operational sequence that defines the environment, duration, and how the system architecture protects the critical functions implemented in electronics. Assurance involves not only the quality of the parts, but also their specific application and installation.


To ensure that electronics failures do not become a significant risk driver overtaking the high risks in ascent propulsion and landing systems, including parachutes requires careful consideration of system architecture, backup systems, and the assurance program.

From an overall mission perspective, one strategy might suggest the biggest contributors to mission risk should result in the best that can be achieved with non-avionics system elements, such as crew life support, engines, entry thermal protection, and landing systems. In other words, electronics should not surface as a mission risk driver. Established techniques can dramatically improve the reliability of electronics; however, there are limited ways to dramatically improve the reliability of non-electrical elements, such as parachutes.

Figure 5.0-1. Notional Non-Electrical and Electrical Failure Rate Contributors to Loss of Mission



Assuring electronics risk does not drive mission risk by more than 1 to 10 percent implies electronics is at least 10 if not 100 times less of a contributor to overall mission risk than non-electronics elements. Figure 5.0-1 shows how a notional 1 in 200 non-electrical probability of

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 11 of 43 |

failure combines with a 1 in 20,000 rate to result in a system failure of 1 in 198. In this example, the electrical system degrades the predicted mission failure rate by 1 percent.

The term “commercial off the shelf parts” or “COTS” is broadly defined and not applied consistently. Often the medical, automotive, commercial aviation, and some consumer electronics industries are labeled as commercial. These industries often control their supply chain. Because their products such as cars or cell phones are sold to consumers does not mean they use commercially available parts without controlling their source or subjecting their supply chain to some kind of qualification or screening program. On the other hand, other commercially-available consumer parts do not follow any specific qualification or screening processes.

A *qualitative assessment* showing the system effects of parts quality can be achieved by applying relative failure rate factors described in Table 5.0-1. The table compares the definition of parts grades and identifies a relative parts failure rate factor that can be used to compare parts programs. These factors can be obtained from the NASA Electronic Parts and Packaging (NEPP)¹. Fundamentally it indicates: Grade 2 active parts are four times more likely to fail than Grade 1 parts; screened MIL-883 parts are eight times more likely to fail than Grade 1 parts; unscreened commercial parts 40 times more likely than Grade 1, or 10 times more likely than Grade 2. By their nature, these relative failure rates are not meant to be precise nor applicable to all parts. Data supporting the approximate value of the relative failures rates is presented in Appendix B.

This comparison shows the relative value of screening and production line control programs. The actual parts used from Grade 1 and commercial categories may perform and potentially last the same, but the difference lies in the uncertainty of the higher bound of the failure rate as shown in Figure 5.0-2. Without screening, commercial parts with unknown defects could have variable failure rates peaking over 40 times higher than a baseline Level 1 Established Reliability part type with quantified known failure rates. This risk is compounded by the clustering nature of EEE parts failure modes; that is, it is common to observe parts failures clustered around a manufacturing lot or specific time/facility.

¹ https://nepp.nasa.gov/nepag/info/parts_risk_matrix.htm


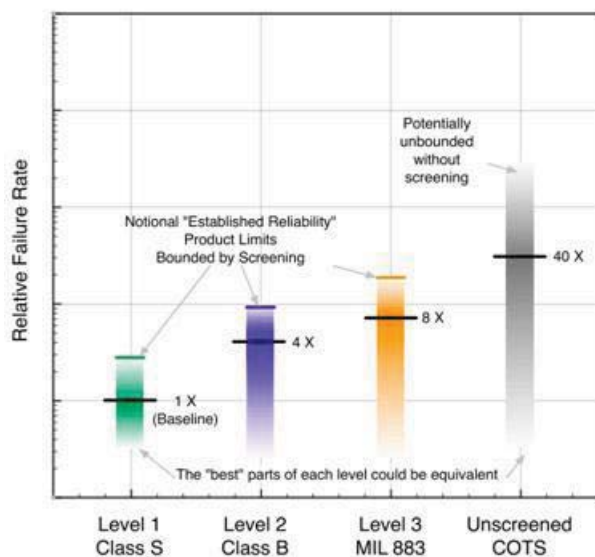

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 12 of 43 |

Table 5.0-1. Comparison of Reliability Factors and Parts Grade (adapted from NEPP¹)

| | | NPSL Level 1, Class S or 975 Grade 1 | NPSL Level 2 Class B or 975 Grade 2 | NPSL Level 3 MIL-883 or Vendor Flow | Unscreened Commercial/ Industrial |
|---|---------------------------------|---|---|--|---|
| Microcircuits, Active Parts (microcircuits, transistors diodes, etc.) | Relative Failure Rate Factor | 1 | 4 | 8 | 40 |
| | | MIL JAN Class S MIL QML Class V MIL QML Class K “S” SCD ESA/SCC Level B JAXA QPL/QML Class I | MIL JAN Class D MIL QML Class Q MIL QML Class H MIL JANTXV, JANJ ESA/SCC Level B JAXA QPL/QML Class II | MIL 883 B MIL QML Class M,N,T MIL QML Class D,E DSCC Drawing | COTS |
| Passive Parts (resistors, capacitors, etc.) | Relative Failure Rate Factor | 1 | 10 | 100 | Unknown |
| | | MIL “S” Failure Rate MIL “R” where no “S” QPL MIL Weibull “C” (“D” id available) MIL-PRF-38535 Class S, T ESA/SCC Level B JAXA QPL/QML Class I | MIL “P” Failure Rate ESA/SCC Level B JAXA QPL/QML Class II | MIL “M” or “L” Failure Rate DSCC Drawing | COTS |

Figure 5.0-2. Notional Parts Failure Rate and Uncertainty about Median



| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 13 of 43 |

6.0 Review of Commercial Crew Provider Rationale for using Commercial Parts

According to the NESC request (refer to Appendix A), at least one CCP partner expressed an interest in using parts procured from a commercial online distributor using the industrial grade (due to desired performance over expanded temperature range compared to commercial grade), and to perform little to no screening or testing on the component at the piece part-level before installation on the board or assembly. The rationale to support this approach, as indicated in the NESC request, is listed below in italics along with some considerations and comments by the NESC Avionics TDT:

1. *Extensive testing at the board and box-level equates to some portion of the testing required to be classified as a higher grade part.*


Board-level testing is far less perceptive than part-level testing in identifying weak parts susceptible to premature failure. Furthermore, board- and box-level testing does not necessarily demonstrate part-level performance margin. Board- and box-level testing is valuable to verify overall functional performance and to identify gross functional failures induced by assembly defects.

Board testing cannot screen for each part's parametric performance and stability at a part's design limit. Part-level testing is most perceptive in identifying the weak parts by exercising the part at voltage, current, temperature extremes, and other environmental factors not possible at the board level. A board can function during test, but have near zero margin due to circuit design flaws and/or a latent part flaws and this would go undetected. Margin against unexpected environmental conditions makes for a robust design.

A box-level elevated temperature burn-in does not screen for failure modes not activated in a way predicted by the Arrhenius behavior. Some failure modes are activated and accelerated when parts operate closer to voltage and current limits and such conditions are often not possible in circuits at higher levels of integration. The lowest part rating on the board limits the allowable temperature excursion to preclude overstress.

Reliability models such as MIL-HDBK-217 are based on the Arrhenius theory that part degradation mechanisms such as internal corrosion due to contamination approximately double in rate every 10 degrees centigrade and on an assumption that system reliability is predictable because parts fail from wear-out. It is the NESC team's experience that most part failures are from defects introduced by manufacture or handling, from misapplication, or from design flaws and not from wear-out mechanisms, such as semiconductor die metal migration or oxide layer thinning over time.

Uncontrolled manufacturing design changes and uncontrolled construction of the die could affect performance near operational limits (e.g., voltage, temperature, current, propagation

| | | | |
|---|---|---|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 14 of 43 |

delay, etc.) or under total dose and single event upset radiation environment. See item 4 below for further discussions about uncontrolled manufacturing process changes.

2. *Their architecture, which is dual failure tolerance at the system-level as well as internal to the avionics boxes, is robust to failures.*

Robustness implies a predictable response under unanticipated or unknown failure mechanisms and thus provides the ability to continue the mission. Robustness would depend on board/system architecture, whether the failure cause/mechanism is generic, and whether the mission is long enough for multiple failures to occur.

Multiple strings can defend against random failures, but the NESC team's experience is that most failures are not truly random in nature. Many failure causes are correlated to multiple parts within a lot. Part- or board-level manufacturing processes or handling can introduce latent defects in multiple parts. Also, common environments such as radiation, thermal, and vibration can cause failures across all strings over time (i.e., common cause failures (CCF)).


Robustness involves margin to physical limits. Without testing of parts at or near their operational limits, little is known about the parts margin in circuit. Robustness also involves application of the parts in a manner providing margin to data sheet limits (derating) so the system can survive unexpected or unforeseen events.

3. *The overall increase in failure rates given these lower grade parts, when this 3-string architecture is considered, does not appreciably increase loss of crew (LOC) or loss of mission (LOM).*

When the electrical elements do not appreciably affect the overall system reliability (less than about 1 percent), it implies the electrical system is about 100 times less likely to fail than the non-electrical elements. However, examining a notional system indicates that commercial parts failure rates (see Table 5.0-1) could have a dramatic impact on the total system failure probability for missions 2 weeks in duration or longer. Mission duration is a big driver in these results and poor quality parts can drive risk in the electrical elements far above the non-electrical with significant impact to the total system failure rate. See Section 7.2.

4. *The use of commercial parts means a greater part selection with more nimble part lines which generate higher performing parts (higher millions of instructions per second (MIPS), lower resistances drain to source (when) on (RDSon), etc.), which offsets failure rates as performance margin is increased.*

Higher performance does not necessarily equate to a reliability improvement. Higher performance is most often functional and not measured against margin to environmental stresses that affect the part in the system, such as its susceptibility to electrostatic discharge (ESD), transients, or radiation damage. Higher performing parts could exhibit higher failure

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 15 of 43 |

rates in a real system. For example, higher performance and higher speed parts with smaller feature sizes or thinner oxides might be more susceptible to ESD, transients, or radiation damage. There is some anecdotal evidence indicating that reliability is worse because reduced feature sizes result in reduced operating margins to time-dependent physics of failure limits (e.g., electromigration, and dielectric breakdown).²

Nimble part manufacturing lines allow a manufacturer to meet changing market demands. These changes can affect manufacturing locations, facilities, materials, processes, and procedures. These, in turn, can unintentionally worsen performance relative to environmental factors not covered by typical data sheets, such as susceptibility to radiation damage. Without source control drawings or other techniques to manage the supply chain, parts changes can affect system reliability.

Nimble or uncontrolled part lines can lead to changes in parts or discontinuance and replacement making the original electronics design that relied on them obsolete (parts obsolescence).

5. *In addition to performance, their designs can employ newer technologies not available in the Class S Grade 1 versions.*

New technology can be a benefit if it results in a significantly simpler system with fewer parts or less complexity, less power, and cooler operation. However, newer technology comes with risks and unexplored problems. For example, the newer RDSON field effect transistors (FETs) also bring with this change the possibility of thermal runaway when applied in circuits requiring operation in the linear region for periods longer than 10 milliseconds³.


6. *The obvious gains in schedule and cost trades.*

Programmatic gains in schedule or cost do not necessarily correlate to improved reliability or safety relative to the parts assurance program and can completely evaporate in a single anomaly and recovery. A paper written by Sampson and Plante⁴ describes the Goddard Space Flight Center's (GSFC) experience with cost drivers on parts programs.

² Does Silicon Wearout: An OEM's Perspective, Dr. C. Hillman; <http://www.ewh.ieee.org/r6/scv/rl/articles/Does%20Silicon%20Wearout.pdf>

³ Problem Advisory Linear Mode Application, Power MOSFET #FV5-P-09-01A, 23 April 2009

⁴ Cost Impacts Due to Electronic Part Upgrading for Use in NASA Programs, Jeannette Plante, Dynamic Range Corporation, Michael J. Sampson, NASA Goddard Space Flight Center, 3/6/2003

| | | | |
|---|---|---|----------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 16 of 43 |

7.0 Response to Commercial Crew Program Specific Requests of the NESC

The original request, provided in Appendix A, asked for answers to the questions shown in italics below. Responses to the questions by the NESC Avionics TDT are provided following the request/questions.


1. *Provide back to the CCP Engineering leadership a benchmark on EEE parts selection criteria from commercial aviation large and small (Boeing-Seattle and Cessna or equivalents). It is understood that the mission duration as well as natural and induced environments are different. However, this data point may help program decision-makers frame this risk.*

Various industries use different approaches. Aircraft, automotive, and some consumer electronics industries typically apply supply chain management processes to assure the parts built into the end product are of the quality needed to perform their intended function and mission. In other words, they have an assurance program with parts vendors. The NESC team looked at aviation and automotive approaches. The CCP team can perform further research of supply chain management and assurance processes for other industries.

Automotive Industry. The automotive industry has an extensive supply management program and relationship with their suppliers as do some, but not all, consumer electronics suppliers. Commercial industries typically give emphasis to parts quality and changes because of the impacts of recalls and warranty returns. Parts are often purchased to a source control drawing with a unique part number, and are purchased directly from the manufacturer or for commodity items such as simple passive resistors or capacitors at least from a manufacturer's authorized supplier. Monitoring of suppliers and restrictions on approved suppliers is common. The automotive industry uses a Production Part Approval Process (PPAP⁵). EEE parts suppliers have special processes to meet the requirements for the automotive industry. Manufacturers take supply chain management seriously. Not only do they assure the quality of the parts, they also actively monitor their supplier's business health. They perform "design failure modes and effects analysis (FMEAs)" and "production process FMEAs" to identify potential ways faulty parts might enter their end item products.

2. **Commercial Aviation.** The Federal Aviation Administration predicts the number of commercial aircraft to grow from 7,816 in 2007 to 12,202 in 2025. As a result, the Boeing Company and Airbus, have reported that only those avionics suppliers with an International

⁵ <http://www.aiag.org/staticcontent/quality/index.cfm> The Automotive Industry Action Group, also known as AIAG, manages the Production Part Approval Process (PPAP) standards.

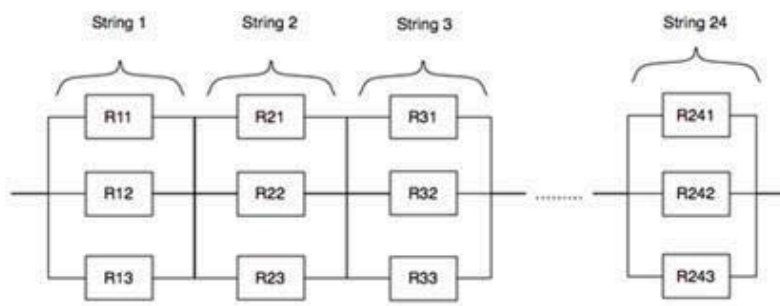
| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 17 of 43 |

Electrotechnical Commission (IEC) certified Electronic Component Management Plan (ECMP) need apply. IEC Technical Specification (TS) 62239 provides a standard format in which suppliers can document processes, including part selection, application and qualification, quality assurance, dependability, as well as data and obsolescence management. Boeing and Airbus have notified supply chain associates that starting with their 787 and A350 models, respectively, suppliers must comply with the IEC TS 62239 standard for the preparation of an ECMP. These plans are critical to assuring the reliability, sustainability, and suitability of the COTS electronic components used in today's avionics systems.⁶ *Given a generic architecture with dual redundancy across all elements, an assumption that common parts exist in each string, a typical division of LOC/LOM allocation to avionics, can move from Grade 1/Class S parts to Commercial/Industrial parts with no upscreen really have little effect on overall LOC/LOM? A notional analysis is requested to assess this assertion.*

This question is difficult to answer with any meaningful accuracy or precision. There is neither a "generic architecture" nor is there a "typical division" of failure rate between electronics and non-electronics. There is also no all-encompassing generic mission profile that includes natural and induced environments.


One strategy is to guide the electronics design to a failure rate of less than 1/10th of the non-electrical system elements, such as the parachutes, heat shield, and engines. In this case, the system reliability is not markedly improved with improvements in the electronics reliability. As the failure rates of the electronics approaches 1/10 of the non-electrical, the total system failure rate dramatically increases as shown in the table and plots below.

Figure 7.2-1. Notional Electronics System Architecture: 3 Cross-Strapped Strings of 24 Boxes



A notional electronics architecture that is used for the relative comparisons is shown in Figure 7.2-1. It consists of 24 cross-strapped series system elements (avionics boxes) each with a baseline failure rate of 2^{-6} per hour assuming a Grade 1 Class S parts program. The

⁶ Distribution Insider, An Industry Guide to Electronics Supply and Demand, Commercial Aviation Needs a Plan, 2009.

| | | | |
|---|---|---|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 18 of 43 |

origination of the 24 boxes and the selection of a typical average failure rate was detailed in the NESC's Smart Buyer study⁷.

Figure 7.2-2 notionally shows how parts grade can affect system failure probability. The source of the relative parts failure rate is the NASA NEPP¹ summarized in Table 7.2-1 and Table 7.2-2. The floor of the plot is set to a constant 0.5 percent representing a 1-in-200 chance of the non-electrical system elements failure. The failure rate of the non-electrical system is driven by items, such as parachutes, heat shields, and engines. In this notional example the electrical system failure rate adds to the non-electrical.

As shown in the figure, a triple redundant system with 24 cross strapped elements built with Grade 1 or Class S parts on a 6-month mission contributes 1:66,000 to the overall failure probability, degrading the total system from 1:200 to about 1:198. For an electrical system to degrade the total system by only 1 percent the electrical elements would need less than a 1:20,000 failure probability as shown in Figure 7.2-2.

Class B parts with a 4x Class S failure rate contribute more to the system failure probability, but remain less than the non-electrical portion as shown in Figure 7.2-2. The use of MIL-883 parts with an 8x Class S failure rate, when used in the team's notional system, exceeds the non-electrical failure rate significantly (1:140 vs. 1:200), driving the total system failure rate to 1:84, thus increasing the total system risk (see Table 7.2-1). Use of unscreened commercial parts with failure rates larger than 883 parts (the rate 40 is times higher than Class S parts, per Table 5.0-1) results in dramatically higher failure probabilities as the plot in Figure 7.2-2 shows.

Acquiring commercial parts without an assurance program could result in large uncertainty bars in failure rates, Figure 5.0-2. MIL Established Reliability (ER) parts have data that substantiates their failure rates. Without screening data or an assurance program, there might be little confidence in any type of numerical analysis. Commercial parts could perform as well as a Class "S" part or they could fail prematurely due to "walking wounded" escapes not caught in board- or box-level testing waiting for the right combination of voltage, temperature, mechanical, or operational conditions to fail. Lastly, many flight failures have occurred due to excessive stresses introduced by either the design, or manufacturing and test processes, or interactions with the specific environment or mission profile that are not anticipated by a failure rate analysis or probabilistic risk assessment (PRA) rather than wearout.

⁷ Crew Exploration Vehicle "Smart Buyer" Design Team Final Report, May 2006, section 4.1.4.1 page 182. Copies of the report can be requested from the NESC.


| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 19 of 43 |

Figure 7.2-2. Failure Probability for a Hypothetical 24-Element, 3-String X-Strap Electronics System versus Parts Grade for 6 Months

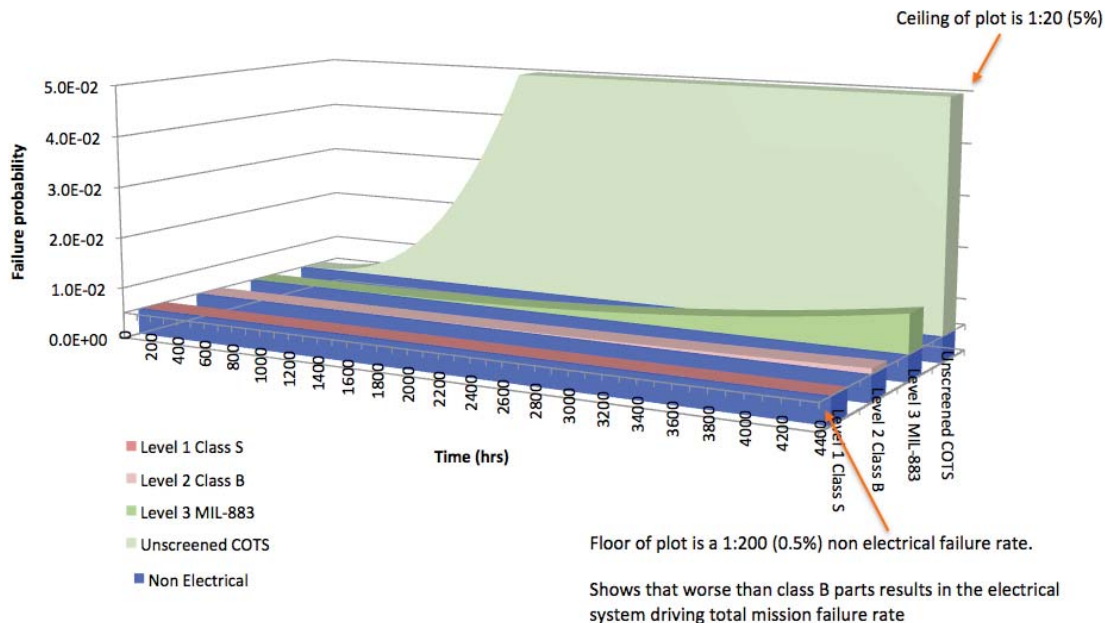


Table 7.2-1. Failure Probability at 6 Months for a Hypothetical 24-Element, 3-String X-Strap Electronics System versus Parts Grade

| | Failure Rate 1:n Flights | | |
|--|--------------------------|-----------------|--------------|
| | Electrical | Non- Electrical | Total System |
| Electrical Contribution 1% of Total for 1:200 | 1:20,000 | 1:200 | 1:198 |
| Electrical Contribution 1/10 of Non-Electrical | 1:2,000 | 1:200 | 1:182 |
| “Notional” System Results: 6 Months | Electrical | Non- Electrical | Total System |
| Baseline Failure Rate Class S | 1:65,400 | 1:200 | 1:199 |
| 4x Failure Rate Class B | 1:1,060 | 1:200 | 1:169 |
| 8x Failure Rate Mil-883 | 1:140 | 1:200 | 1:84 |
| 40x Failure Rate COTS | 1:2 | 1:200 | 1:2 |


| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 20 of 43 |

Figure 7.2-3. Failure Probability for a Hypothetical 24-Element, 3-String X-Strap Electronics System Powered Down After 2 Weeks versus Parts Grade

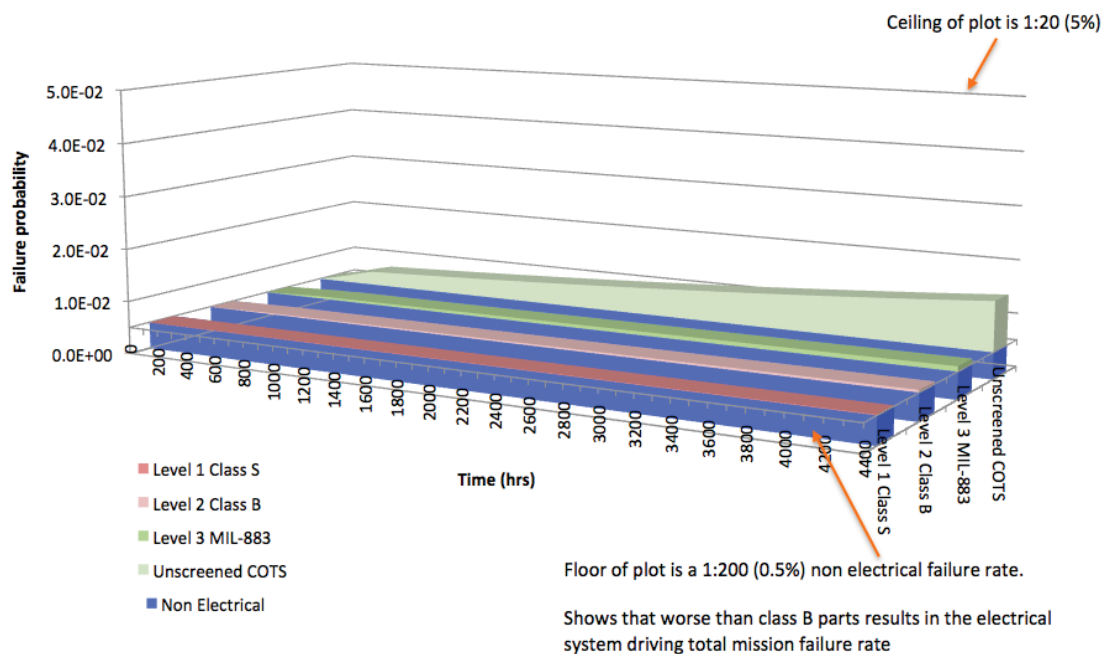



Table 7.2-2. Failure Probability for a Hypothetical 3-String X-Strap Electronics System Powered Down After 2 Weeks versus Parts Grade

| | Failure Rate 1:n Flights | | |
|--|--------------------------|-----------------|--------------|
| | Electrical | Non- Electrical | Total System |
| “Notional” System Results: 6 months, powered off after 2 weeks | | | |
| Baseline Failure Rate Class S | 1: (1:>1,000,000) | 1:200 | 1:200 |
| 4x Failure Rate Class B | 1:186,000 | 1:200 | 1:200 |
| 8x Failure Rate ”MIL-883” | 1:23,500 | 1:200 | 1:198 |
| 40x Failure Rate COTS | 1:200 | 1:200 | 1:101 |

| | | | |
|---|---|---|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 21 of 43 |

3. *Given failure rates collected in Grade 2 upscreens (particle impact noise detection (PIND), X-ray, burn-in, etc.) and data from manufacturers and the field centers, can this assessment team recommend an upscreen/testing regime that would improve the analysis in two such that the LOC/LOM with commercial grade parts approaches that calculated when Grade 2 (Class B, etc.) parts are used?*

Screening of commercial parts to meet Grade 2 parts program requirements is described in several sources including EEE-INST-002. Upscreening commercial parts often results in increased costs over procuring Grade 2 parts from the outset⁴.

In general, there are not sufficient screening failure rate statistics easily available to accurately and quantitatively characterize the different defect rates among the different parts grades. However, there are some qualitative indications.


The team's GSFC experience is that few lots fail the percent defective allowable (PDA) limit, which is 10 percent for Level 2 and 5 percent for Level 1. PDA is the total number of failures allowed from pre-burn-in to post-burn-in electrical. The first indication for a "bad" lot is exceeding its PDA. Commercial lots, which have never been screened, fail PDA more often than MIL parts on a manufacturer's Established Reliability product line. Rarely do ceramic/metal hermetic, 883 type parts suffer lot failures, since most have already seen some level of screening.

When requested at time of purchase, attribute data including screening fallout is supplied with a lot of military grade parts. Military grade part procurements are typically limited to a certificate of compliance. The customer does not receive attributes data for commercial parts and Certificates of Compliance generally lack proper traceability.

There are significant differences in acceptance criteria between commercial and military grade parts leading up to lot qualification and successful destructive physical analysis (DPA). These differences can lead to lot failures in commercial parts that are caused by problems that have been screened from lots of military parts.

Additional testing of commercial parts after their receipt subjects the parts to additional handling. There is considerable expense to develop test fixturing and Automated Test Equipment software for the purposes of screening and qualifying lower grade parts. There is also the possibility of electrical and/or mechanical overstresses (such as ESD or cracked hermetic seals, etc.) due to all the additional handling during the various tests. Often, the total cost is far higher than the difference in piece part cost between commercial and military grades.

Often manufacturer's "warranties" of commercial parts are voided by screening. In some cases, the temperature range had to be reduced to accommodate the limited temperature limits acceptable to the lot. The manufacturer does not guarantee shifts in performance parameters if the screening temperature exceeds their recommend operational temperature

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 22 of 43 |

range. Typically, the plastic encapsulated microcircuit (PEM) devices are rated from 0^C to 70^C. However, to qualify them for spaceflight environments, the test exposure needs to range from -55^C to 85^C or 125^C. The encapsulation of plastic devices is getting better so the gap between using ceramic versus plastic parts is reducing. However, projects still have to deal with delamination and possible ionic contamination, depending on control of the cleaning process.

Hybrid and multichip modules introduce additional risk into electronic systems if the components and assembly techniques are not controlled. The issue is that post-assembly tests cannot assure quality or long-term reliability since production quantities are smaller. Assembly techniques such as die/parts placement, soldering, and wire bonding should be verified. Also, individual components cannot be stressed as they would if they were screened before assembly into the module. Examples of such devices are hybrid direct current to direct current (DC/DC) converters, solid-state power switches, analog to digital (A/D) converters, and stacked memory modules.

Some noteworthy qualitative differences between commercial and high reliability military parts based on team experience are listed in Table 7.2-3. Screened military parts and unscreened commercial parts are potentially different. It is up to the program to explore such differences, understand what the differences might mean to safety and reliability, and then defend against those undesired effects. Defenses could range from obviating the risk, diverse backups, or different parts.

- a. *Please provide a primer of parts grades and associated testing of each along with an assessment of what tests provide the greatest value.*

The NESC team's opinion is that no single prescription or single approach will provide an optimum answer for all parts in a complex system composed of safety critical and non-critical functions.

The NESC team recommends that the parts program be engineered, planned, and implemented in concert with a top-down mission assurance program. Resources, such as EEE-INST-002, provide a source for the various parts screening activities.



| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 23 of 43 |

Table 7.2-3. General Comparison of MIL versus COTS EEE Parts for High Reliability Applications

| Parts Characteristic | | Parts Quality Spectrum | |
|----------------------|--|---|--|
| | | Space / MIL | Unscreened Commercial |
| Intended Use | High Volume | No | Yes |
| | Harsh Environment? | Yes | Maybe to No |
| | Radiation Environments | Yes (if required) | No to rarely |
| | Extreme Temperatures | Yes | Maybe to No |
| | Temp Cycling | Yes | Maybe (but usually to lower levels than MIL) |
| | Vibration/Shock | Yes | Sometimes |
| | Vacuum Pressure | Yes | No |
| | Long-Life | Yes | No (warranty 6 mos to 2 years)? |
| | Failure Rates Tolerated | Very Low | Significantly >> than MIL |
| | Suitable for Mission Critical Applications | Usually | Rarely to Maybe to No |
| Availability | Specification Controlled By... | MIL | Supplier (usually) |
| | Penalties for non-compliance...? | Yes -- Fraud/Fines/Jail | No |
| | Product Lifetime (Obsolescence) | Many Years to Decades | Usually very short (months to few years) |
| | Extensive Variety of Products? | Few | Many |
| | Price | Medium to High | Low to Very Low |
| Construction | User knowledge of internal construction? | Yes, controlled | Rarely |
| | Lot Homogeneity? | Yes | Varies |
| | Designs | Very Stable, Conservative Margins | Supplier Controlled, Aggressive Margins |
| | Materials | Very Stable, Conservative Margins | Supplier Controlled, Aggressive Margins |
| | Processes | Very Stable, Conservative Margins | Supplier Controlled, Aggressive Margins |
| | Size | Bigger | Smaller |
| | Weight | Heavier | Lighter |
| | Changes to Design/Materials/Process | <i>MIL-monitored</i> | Supplier controls changes, May vary frequently |
| Testing | "Established Reliability?" | Available for Passives and some actives | No |
| | Screening | MIL controlled, High Levels | Supplier Controlled, Limited Insight |
| | Qualification | MIL controlled, High Levels | Supplier Controlled, Limited Insight |
| | Requalification | MIL controlled, High Levels | Supplier Controlled, Limited Insight |
| | Harsh Environment? | MIL controlled, High Levels | Not typically designed for harsh environments |
| Device Performance | Functionality | Lower | Higher |
| | Speed | Lower | Higher |
| Miscellaneous | Manufacturing facility location known? | Yes, controlled | Possibly Yes, but often No |
| | Govt Audits? | Yes (typically 2 to 3 year cycle) | No |
| | Support with Problem Investigations? | Yes | No |
| | Potential for Counterfeiting | Lower | Higher |

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 24 of 43 |

4. *How does the short mission durations play into the analysis above and does the analysis support a different answer between launch vehicle and spacecraft?*

The details of the mission are a significant driver. Mission durations of 2 hours, 2 weeks, and 6 months yield dramatically different results. Using the notional three-string cross-strapped system architecture described above, 2-hour missions are not significantly affected by parts quality; however, 6-month missions are significantly affected. In addition to mission length, the configuration of the electronics drives the system failure rates. For a 6-month mission, failure rates are dramatically reduced if the electronics is powered down after 2 weeks should the system be docked to the International Space Station (ISS) for the remaining 5-½ months as shown in Figure 7.2-3. Compare the Figure 7.2-3 power down case to the powered for 6-month case shown in Figure 7.2-2. For this notional example, a failure rate of 1/10 the powered failure rate is assumed while powered down.

See Table 7.2-4, Table 7.2-5, and Figure 7.2-4.

Table 7.2-4. Progression of Failure Probability Considering Mission Length for a Hypothetical 24-Element, 3-String X-Strap Electronics System versus Parts Grade

| | Notional System Level Failure Rate 1:n missions (1:n Electronics Failure Rate) assuming a 1:200 non-electrical failure rate in series | | | |
|-----------------------------------|---|----------------------------|----------------------------|--------------------------|
| Mission | Class S Baseline Failure Rate | Class B 4x Failure Rate | MIL-883 8x Failure Rate | COTS 40x Failure Rate |
| 2 hours | 1:200 (1:>>>1,000,000) | 1:200 (1:>>>1,000,000) | 1:200 (1:>>>1,000,000) | 1:200 (1:>1,000,000) |
| 2 weeks | 1:200 (1:>>>1,000,000) | 1:200 (1:>1,000,000) | 1:200 (1:270,000) | 1:184 (1:2,200) |
| 6 months, unpowered after 2 weeks | 1:200 (1:>1,000,000) | 1:200 (1:186,000) | 1:198 (1:23,500) | 1:101 (1:200) |
| 6 months powered | 1:199 (1:65,400) | 1:169 (1:1,060) | 1:84 (1:140) | 1:2 (1:2) |

Figure 7.2-4. Failure Probability for a Hypothetical 24-Element, 3-String X-Strap Electronics System for a 2-Week Mission versus Parts Grade

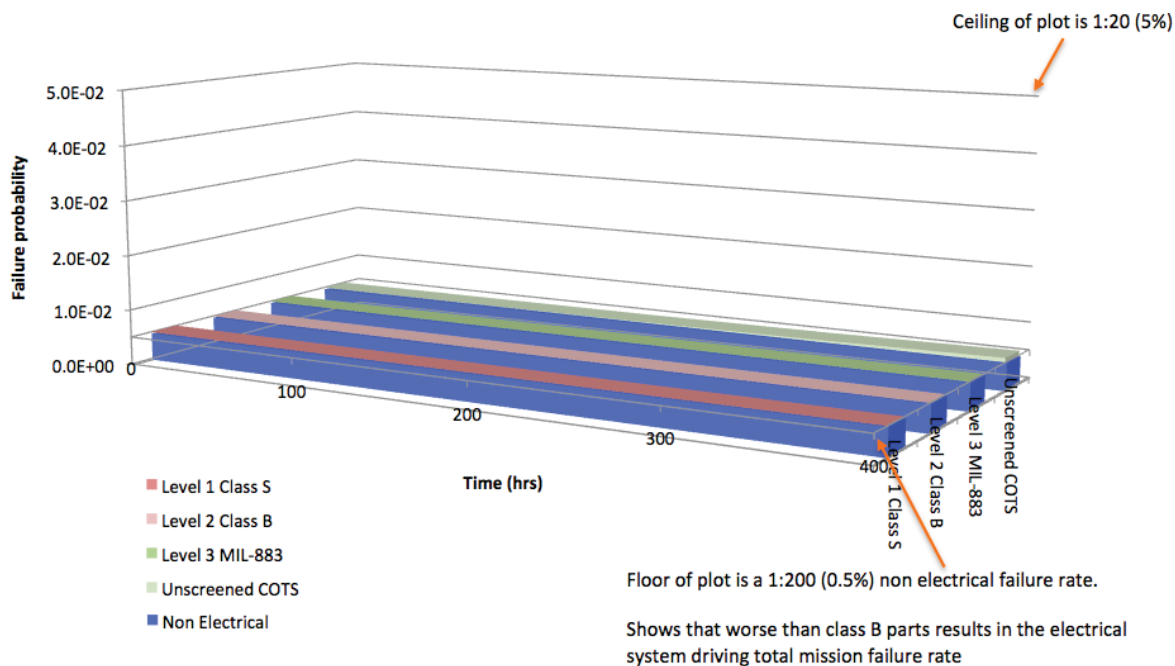



Table 7.2-5. Failure Probability for a Hypothetical 24-Element 3-String X-Strap Electronics System for a 2-Week Mission versus Parts Grade

| | Failure Rate 1:n Flights | | |
|------------------------------------|--------------------------|----------------|--------------|
| | Electrical | Non-Electrical | Total System |
| “Notional” System Results: 2 weeks | | | |
| Baseline Failure Rate Class S | 1:>>1,000,000 | 1:200 | 1:200 |
| 4x Failure Rate Class B | 1:>1,000,000 | 1:200 | 1:200 |
| 8x Failure Rate MIL-883 | 1:270,000 | 1:200 | 1:200 |
| 40x Failure Rate COTS | 1:2,200 | 1:200 | 1:184 |

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 26 of 43 |

5. *How does (sic) CCFs play into the results? Given the likelihood of similar strings, and hence similar parts in similar lots across all the legs of redundancy, does common cause dominate the analysis results?*

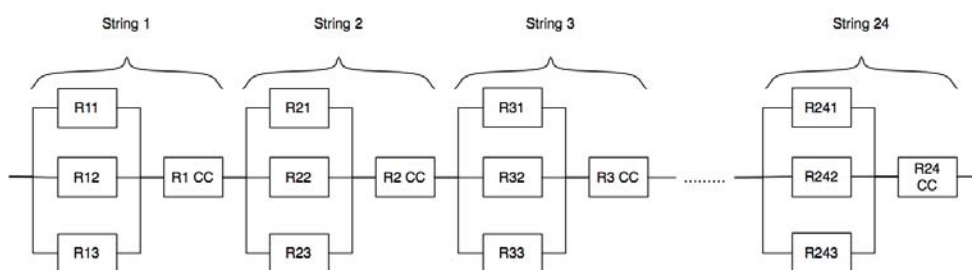
A CCF leads to the system failing to perform its intended function due to a systematic fault in the design or implementation of a system, or a natural or induced stress leading to a premature failure of redundant elements within one mission lifetime. Common stresses can include environments such as thermal, vibration, and radiation and/or electrical voltage or current stresses propagating from a single failure. Since CCFs can affect multiple redundant elements in a system, the probability of CCFs can become the dominant factor in the overall probability of failure.


A CCF occurs when a single fault or condition results in functional failures of multiple components. CCFs are hard to predict and are driven by common environments encountered by redundant components during the mission, as well as manufacturing techniques and processes, handling, and other factors. The frequency of CCFs is difficult to estimate. However, modern process-driven production techniques can introduce common failure modes or weaknesses into multiple copies of parts, boards, and electronics boxes. The modeling techniques and available failure rate data make the predictive calculations of these failures cumbersome and the results obtained questionable.

One of the simplest and most practical techniques to estimate CCFs is the beta factor, β , approach. This approach assumes that the total failure rate of a system is composed of a random or independent failure rate plus a common cause or dependent failure rate, $\lambda_{\text{total}} = \lambda_{\text{independent}} + \lambda_{\text{common cause}}$. The β factor is used to calculate the CCF rate $\lambda_{\text{common cause}} = \beta * \lambda_{\text{independent}}$.

The modeling technique used for the notional example utilizes the β factor to represent the conditional probability that if one component fails, other like components will fail and is modeled as an element in series with a parallel set of redundant components as shown in Figure 7.2-5.

Figure 7.2-5. System Diagram Showing Random and CCFs



| | | | |
|---|---|--|----------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 27 of 43 |

The series element titled as R1 CC represents the redundant element #1 CCF probability. Three β factors, low medium and high, are compared in Table 7.2-6. The β factors consider the probability of the first string failure also causing a second string failure and then the probability of the second string failure also causing the third string failure. For the low β of 3^{-6} , 1 out of every 333 thousand failures of one element also results in the failure of all three. It was assumed that 1 out of 1000 failures (0.1 percent) of the first string failures also cause the second string to fail and then 3 out of 1000 second string failures (0.3 percent) also cause the third string to fail. For the medium β of 300^{-6} , it was assumed that 1 out of 100 failures (1 percent) of the first string also causes the second string to fail and then 3 out of 100 second string failures (3 percent) cause the third string to fail. For the high β of $3,000^{-6}$, it was assumed that 3 out of 100 failures (3 percent) of the first string also cause the second string to fail and then 10 out of 100 second string failures (10 percent) also cause the third string to fail.

In the simple notional example shown in Figure 7.2-6 and Table 7.2-6, common cause is not the major driver when considering unscreened COTS parts with a factor of 40 increase in random failure rate. The inherent failure rate of the parts themselves for the mission duration predominates. However, for high reliability parts the system failure rate does depend on the CCFs. For the low β factor there is little effect even for the high reliability Level 1 parts. Medium β results in more significant effects in the high reliability Level 1 parts. However, a parts failure rate factor of 40 for the unscreened COTS is large and dominates even the higher common cause β factors.


| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 28 of 43 |

Figure 7.2-6. Failure Probability for a Hypothetical 24-Element 3-String X-Strap Electronics System with CCF of 1 percent for 2nd String and 3 percent for 3rd String versus Parts Grade over a 6-Month Mission

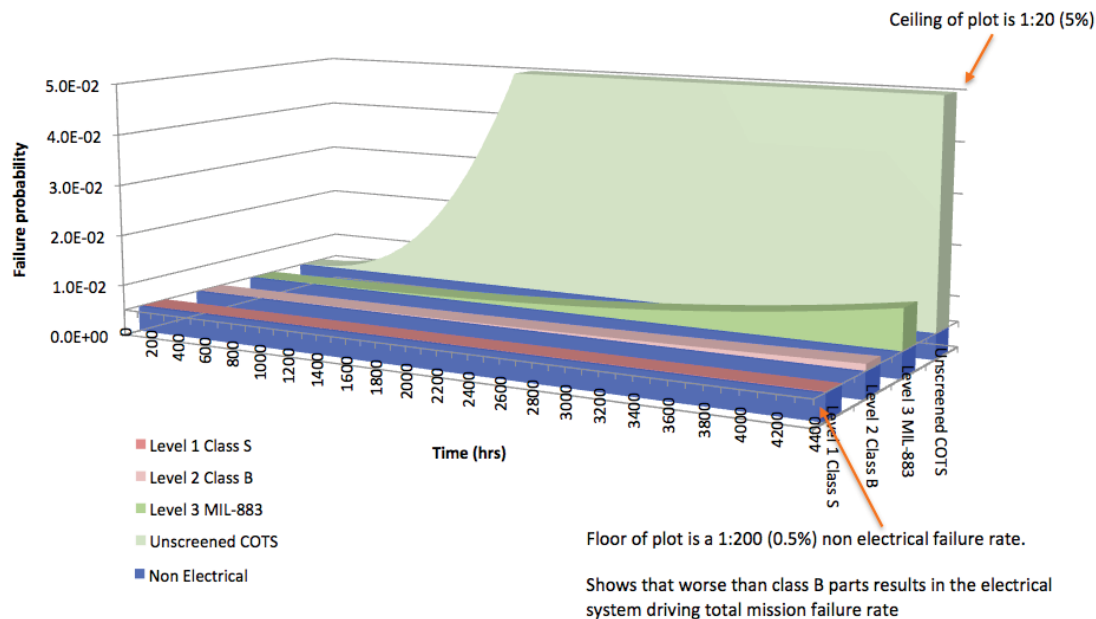



Table 7.2-6. Failure Probability for a Hypothetical 3-String X-Strap Electronics System with Various CCF Rates versus Parts Grade over a 6-Month Mission

| | System Failure Rate 1:n (Electronics Failure Rate 1:n Flights) assuming 1:200 non electronics failure rate | | | |
|-------------------------------|---|----------------------|---------------------------|---------------------------|
| “Notional” System Results: | Baseline: No CCF | Low $\beta = 3^{-6}$ | Medium $\beta = 300^{-6}$ | High $\beta = 3,000^{-6}$ |
| Baseline Failure Rate Class S | 1:199 (1:65,400) | 1:199 (1:62,900) | 1:197 (1:12,900) | 1:178 (1:1,580) |
| 4x Failure Rate Class B | 1:168 (1:1,060) | 1:168 (1:1,060) | 1:162 (1:844) | 1:119 (1:296) |
| 8x Failure Rate MIL-883 | 1:82 (1:140) | 1:82 (1:140) | 1:80 (1:132) | 1:59 (1:84) |
| 40x Failure Rate COTS | 1:2 (1:2) | 1:2 (1:2) | 1:2 (1:2) | 1:2 (1:2) |

| | | | |
|---|---|---|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 29 of 43 |

8.0 Can COTS EEE Parts Be Used in Flight Hardware Systems?


In general, a parts assurance program guides proper control of risk through the design, derating, qualification, screening, implementation, and traceability of parts to ensure they will perform as intended. Parts become flightworthy when they are a product of an assurance program targeted to control risk. Table 8.0-1 identifies critical elements of a parts assurance program.

Table 8.0-1. Assurance Program Elements for Assuring Flightworthy Parts

| Elements | Description |
|---------------------------------------|---|
| Application (design & implementation) | Proper in circuit use and protection from credible stresses induced by the mission's natural and induced environments. Protection from stresses resulting from failure propagation. Proper implementation and assembly controlling stresses to electrical connections, thermal interface, and vibration loads. |
| Derating | Margin-to-maximum operating limits voltage, current, temperature, mechanical stresses to provide robustness against unexpected stresses, and extend service life. |
| Qualification | Part design and manufacturer's demonstrated ability to deliver a part consistently meeting part performance and operating range requirements consistent with the mission application. Assure the space, launch, and landing environments (including radiation, thermal, vibration, etc.) do not damage or destroy a part that functions properly on the ground. Control of production process and limit unexpected consequences of manufacturer's changes to part design or construction process. |
| Screening | Expose parts to safe electrical performance and environmental limits to accelerate the identification of infant mortals or weak parts with latent defects not possible through board and box- and system-level acceptance tests. |
| Traceability | Maintain record of the source of parts and where they are located within the electronics assemblies. Two-way traceability allows identification of the source of a suspect part and location of similar suspect parts. |
| Counterfeit Control | Prevent the introduction of inferior parts into electronics. Constrain parts to trusted sources. Ability to trace part back to qualified manufacturer. |

Some commercial part technologies that are acceptable for terrestrial use have inherent issues when exposed to the natural or induced space environment. According to published reports, the Phobos-Grunt mission failed "... due to non-space qualified parts being used in some of the electronics circuits." "The Phobos-Grunt failure emphasizes the unforgiving nature of space exploration, where cutting corners in the spacecraft development, especially in testing, can be fatal."⁸ Good gel electrolyte capacitors if non-hermetic will dry out and fail in hard vacuum. Flying unsealed commercial batteries in space would be expected to yield similar results. Vacuum also typically causes parts to run hotter since there is loss of convection cooling. Early

⁸ <http://planetary.org/blog/article/00003361/>

| | | | |
|---|---|--|----------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 30 of 43 |

fuse blowout on a satellite was observed after 9 months since the fuse elements were not sufficiently derated for vacuum use, and ran progressively hotter due to internal loss of air over time leading to open circuit of the fuse elements. Vibration can cause issues with some parts technologies; examples being cPCI connector plating fretting and ball grid arrays solder joint cracking. Radiation from both total dose and single event effects can be an issue for some part technologies. Some parts fail from an integrated dose as low as 500 rads and a number of parts are susceptible to destructive single-event latchups and burnouts. Some of these issues can be mitigated by hermetic packaging, derating, error detection and correction (EDAC), triple mode voting, etc., and some cannot.

A proper control of risk to LOC must be grounded in a top-down assessment of critical functions necessary to accomplish the mission and safely return the crew to Earth. Risk assessments must explore how commercial parts will perform their intended functions, understand EEE parts failure modes, understand system-level impacts should the parts fail at a higher rate, with clear understanding of risks to safe return of the crew, including criticality, likelihood, and uncertainty.


It is the mission that dictates the environmental requirements, the application requirements (including criticality), and the time duration. Thus, the selection of the EEE parts must ensure assurance of compliance to meet these requirements. The environment, application, and overall mission time duration (including the time from the fabrication of the component, through testing, up to the end of life of the mission) in conjunction with an overall reliability analysis, hazard analysis, and FMEAs (or equivalent) will help the program decide which EEE parts grades are to be used.

Any given part class has an uncertainty factor with respect to reliability, and quoted failure rates represent averages. Unfortunately, many part failure modes are clustered in time and do not occur randomly over time, therefore the average rate is not an accurate estimate of the risk. When an EEE part's undesirable failure mode is identified it is paramount for the parts assurance program to provide sufficient traceability to identify and remove other suspect parts. The allowable mission risk and the system design will determine acceptable EEE parts grades and uncertainty in failure rates. A part with higher uncertainty may be used in an application as long as the proper screening is performed on the given part thus reducing the uncertainty level through the detection and removal of outliers.

The top-down assurance program must ensure that the entire mission-driven requirements (e.g., environmental, application, and time) and any other derived and/or additional requirements are met. The following sections describe key characteristics of a parts assurance program.

8.1 Part of an Established Top-Down Assurance Program

For the Human Exploration Programs, it is important to understand the critical functions necessary to accomplish the mission of taking the crew into orbit, and/or the ISS or other

| | | | |
|---|---|--|----------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 31 of 43 |

celestial body and returning the crew safely to Earth, and where proper operation of parts must be supported by test of margin to its limits. For example, both the strength of parachute risers to survive transient loads and EEE parts' capability to fire pyros or non-explosive actuators (NEA) under expected mission environments are important to returning the crew safely to Earth.

In a constrained environment the assurance program should apply its resources where they are most effective. This is only possible when the assurance program is guided by a top-down assessment of the critical functions and how they might fail and what defenses need to be in place.

The top-down assurance program is also critical in controlling CCFs, such as cracked seals, or common electrical over-stresses such as ESD, wire bonding, contamination, etc.

Mission-unique environmental effects including natural and induced thermal, mechanical, vibration and radiation are addressed in the assurance program. Commercial parts especially those pushing the speed and low voltage envelope might be susceptible to radiation effects that are only discoverable by testing. Commercial parts rarely if ever undergo total dose radiation or single-events effects testing.

While not unique to commercial parts, failures are often due to problems associated with application and/or manufacturing issues (at component level as well as at system-level). Adverse impacts to reliability can affect any parts program when insufficient derating or application issues exist. Derating provides margin for unexpected interactions or other surprises. Not only does derating promote long life, but also it allows the system to tolerate unexpected variances in voltage, current, or other critical parameters. Parts stress analysis and worst case analysis backs up any parts program. Engineers need to know where/when parts are being pushed to their margin or limits, and where/when margins are tight or robustness is low.


Lastly, proper assembly techniques are required to avoid workmanship-related threats, such as those that can be caused by hand-soldering of surface mounted parts, etc.

8.2 Mechanism to Confirm Parts Quality

The EEE Parts Program must ensure that the selected components will meet the requirements necessary to accomplish mission objectives. It is critical that the parts perform as intended and that failure rate assumptions used in risk assessments and reliability analysis is supported and bounded by testing.

8.2.1 Control the Supply Chain through Qualification and Screening

Electrical Performance and Electrical Integrity. The idea behind parts-level testing is to force out the failures early in the production flow by extremes at or near the limits (i.e., at a time where there is minimal investment in the part).

| | | | |
|---|---|---|----------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 32 of 43 |

Part-level screening and burn-in removes the weak parts or beginning of life infant mortality assuring the failure rate of screened parts is in the flat portion of the bathtub curve assumed by the reliability analysis. Proper screening would identify weak parts that fail prematurely, thus validating the reliability analysis. Parts “screening testing” subjects parts to stresses close to their limits that most of the time cannot be duplicated at board- and box-levels. Parts screening seeks to identify marginal parts that might fail prematurely. Testing at extremes or close to the limits ensures that weak ones close to the mean are also caught (i.e., including radiation test for the given mission environment).

Testing at higher levels of integration, such as board- and box-level does not duplicate or replace part-level screening, but rather serves as functional and higher level performance verification with less extreme conditions and environments, which are typically limited by the lowest temperature component and the available supply voltage(s).


Furthermore, parts can have significant flaws that are not detectable with the board-level test. Many parametric performance parameters do not matter at the board level, but they are indicative of a part destined to fail prematurely. However, such weak parts that might fail prematurely are found in parts screening near their operational limits. Box-level test therefore cannot duplicate the parts level screening.

Procuring parts under a Source Control Drawing (SCD) can control parts quality especially for certain mission critical items. SCDs can directly or indirectly control manufacturing processes that might introduce unintended or unexpected performance issues should production changes occur.

Mechanical Integrity. EEE parts are typically available in many different type of packages, from ceramic, metal, glass, etc., to plastic encapsulated packages; different footprint and pin arrangements; different types of performing internal connections/bonding as well as the material used, such as gold, aluminum, internal and external coatings, etc. Thus, it is important to understand the effect of manufacturing conditions may have on the given application. Furthermore, it is of extreme importance to understand and screen for typical manufacturing defects given the type of component and the manufacturing techniques/process used to produce the given component (i.e., cleaning processes that may introduce contaminants). Screening techniques used to ensure the mechanical integrity of the EEE components include: X-ray (nondestructive test), DPA, bonding pull test, leak test, PIND test, humidity tests, etc.

8.2.2 Defend Against Counterfeit Parts

Low cost and poorly performing counterfeit parts are increasingly becoming a problem. Counterfeit parts can have dramatic effects on actual or perceived performance and reliability. Counterfeit parts may function in a circuit, but may not have the radiation tolerance or margin against limits. The following links are provided for reference:

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 33 of 43 |

<http://www.c-span.org/Events/Senate-Investigates-Counterfeit-Parts-in-Military-Equipment/10737425339/>

<http://www.businessweek.com/news/2011-11-08/china-counterfeit-parts-in-u-s-military-boeing-l3-aircraft.html>

<http://www.cnn.com/2011/11/07/us/u-s-military-bogus-parts/>

Counterfeit parts might reduce reliability in unexpected ways and might affect multiple strings in an identical fashion (i.e., potentially leading to CCFs). Identifying and controlling the unintended introduction of counterfeit parts requires a parts program that includes traceability and procuring parts directly from the manufacturer or authorized outlet, as well as a proper screening process.


8.2.3 Accurate Assessment of Commercial Parts Failure Rates

“Higher Performance Parts” often have lower margins between operational and failure limits. Modern computer-aided design (CAD) tools used by chip designers allow improved performance and reduced margins to limits. This higher performance does not help reliability especially when margins to limits are reduced. Higher performance can help with lower power/thermal stress or where offsetting reduction in complexity or parts occur. Reducing margins is a byproduct of denser packaging, faster clock speeds resulting in smaller feature sizes, and lower supply voltages; such parts have reduced tolerance to voltage overstress and ESD.

Manufacturers may publish their failure rates for what they expect are known good parts. This is different than the defect rate that is typically unpublished. Defects are typically found in clusters and during screening. Removing the cluster of infant mortality failures has a significant impact on the average failure rate. Without eliminating the weak parts through screening, parts could fail prematurely in-flight and can surface in clusters affecting multiple redundant strings.

It is the NESC team’s experience that wear-out failures and truly random failures during life are quite rare. Many parts failures for all grades of parts can be traced to excessive stresses induced by the design, construction, or the natural or induced environments.

Know the threats introduced by low quality parts/components. For example, the mechanical integrity of electrical connectors: insufficient gold-plating of commercial connectors (such as cPCI and others) could lead to serious electrical contact (intermittence) and/or contamination problems. Typical commercial connectors have a lesser gold-plating on their respective pins/socket contacts than what NASA requires (50 micro-inch gold minimum). Mating and demating of these COTS connectors, including the effect of vibration, may wear off the plating of the related pins leading to potential electrical intermittence and/or contamination (e.g., potential electrical short, or contamination of critical sensors). NASA requires 50 micro-inch of gold plating for these reasons for flight applications. Connectors also can have a “press fit” design where a square pin is forced into a round hole, destroying the plated-through hole.

| | | | |
|---|---|---|----------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 34 of 43 |


Perform evaluation of shelf or storage life. There is the potential for shelf-life issues due to how parts are stored. Contamination and moisture can affect all parts in common ways. Parts handling and storage must adhere to manufacturer-recommended storage and handling conditions. A part's package construction (including pin plating, hermeticity, etc.) can drive unique storage and handling needs.

8.2.4 Manage Parts Obsolescence

Level 1 through Level 3 (MIL) as well as commercial parts may become obsolete and may no longer be produced, although the pace of obsolescence is much more rapid for commercial parts in general. Commercial parts are often part of a rapidly evolving line where the design or construction may frequently change as part of continuous process improvements. Minor adjustments usually only require approval at the line organization level. Major changes are carefully controlled but final approval is by the company's internal change control procedure with concurrence possibly sought from major customers. On the other hand, for military parts, major and minor changes are defined by the specifications and major changes require approval by the Qualifying Activity (Defense Logistics Agency, Land and Maritime), before introduction into the MIL qualified production process. As a minor customer, NASA gets no visibility into commercial process changes unless the manufacturer publicly issues a product change notification. For space grade MIL parts, NASA is consulted on major changes and can provide recommendations to the QA regarding validation testing, process control requirements and final approval. Even for non-space grade MIL parts, NASA usually has insight into significant process changes as NASA is afforded the same rights as a military service in the Defense Standardization Program. Although product evolution is therefore slower for MIL parts than commercial, it gives NASA a lot more time to evaluate changes to reduce the risk for unintended consequences. Changes made to commercial parts, which may have no negative impacts for the applications of their primary customers, can have serious impacts for NASA as radiation tolerance may be drastically reduced or electrical parameters may change in undesirable ways so the part may no longer perform properly in the original circuit. As parts become obsolete and are replaced with newer parts, resulting design changes ripple into the circuit board and box design. These changes can adversely affect the total system not only from a performance perspective, but also from a producibility perspective. The parts program should strive to minimize the chance of obsolescence from adversely affecting safety-critical systems.

8.2.5 Identify Threatening Materials

A mechanism is required to ensure that parts with pure tin coatings do not get into systems where tin whiskers could result in serious failures including failures in multiple strings. Due to restriction of hazardous substances (RoHS) regulations mandating lead-free parts in Europe, many commercial parts are tin-coated. Tin whisker threats need to be factored into the program given the potential for long shelf-life or storage on the ground and the potential for reuse and re-flight.

| | | | |
|---|---|--|----------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 35 of 43 |

Materials such as silicone or nylon can pose an outgassing concern in space applications, but may not be a concern for a manned capsule. It may be appropriate to screen and test materials in a crew cabin to assure compatibility with breathable atmosphere and control of fire hazards.

Commercial plastic parts can absorb moisture that can destroy the part under elevated temperature and vacuum conditions.

8.3 Establish a Plan to Identify and Recover from a Defective Lot

A plan should be developed that deals with parts issues should they surface. For example, if a particular capacitor has a generic issue, then what is the recovery strategy? Is there a way to identify the capacitor's source and where parts from the same source or lot may be installed? If the commercial parts do not have traceability, then what can and will be done once defective parts are installed in electronics?


The pedigree of any parts program is grounded in data capturing the parts history with sufficient fidelity to identify where the part originated and where similar defective parts might threaten the mission. Commercial parts give up traceability and therefore the user does not know when and where the parts were made. If a bad commercial lot is found, without some kind of two-way traceability, it may not be possible to replace all instances of the generic part to preserve the intended reliability. If a generic problem is found, then it may not be possible to identify the location of other suspect parts.

A mechanism for traceability should be established identifying where parts from a specific order or lot are located and then, from a printed circuit board (PCB) perspective, where the parts came from. This two-way traceability allows identification of the extent of parts replacement should a problem be found.

Pictures taken of flight boards with sufficient resolution to show installed parts type, part number, and orientation can provide the ability to confirm configuration after the box is accepted for flight. Photographs can often provide evidence to resolve issues that might surface after the box is closed.

The MIL parts community uses the government-industry data exchange program (GIDEP) alert system to warn other users of suspect parts. The widespread user community provides reliability growth by identifying and communicating escapes that surface in the field. Commercial parts are not the subject of communication among customers and therefore do not benefit from the advantage afforded by the GIDEP.

In the commercial world there is not a standard convention for unique identification of part lots. Commercial parts often do not contain lot identification numbers and when they do, they may not be able to distinguish between parts made at different locations or may actually use different die. So it becomes difficult to implement a thorough two-way traceability program necessary to identify other suspect parts.

| | | | |
|---|---|--|----------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 36 of 43 |

9.0 Conclusions

The fundamental question is whether COTS EEE parts with limited screening can be used in crewed flight systems. The answer hinges on the assessment and control of risks associated with a parts-induced system failure.

The NESC team reviewed and analyzed approaches based on screening parts only through box or system-level testing and concluded that there are fundamental concerns with the rationale (Section 6). The approach is based on procuring commercial parts as received from a distributor without qualification for space or additional screening, and assembling them on circuit boards. Such an approach would result in assembling good parts along with any weak parts, parts with latent defects, and infant mortals into flight hardware with the assumption that board, box, and system-level testing can effectively identify parts that might fail during the anticipated mission lifetime.

The team concluded that board, box, and system-level testing cannot replicate accelerating factors that voltage, current, and temperature stresses provide during part-level screening.

Without bounding parts quality through a parts assurance program, large uncertainties will exist in parts failure rates and therefore system failure rates. In addition, without the controls imposed by an assurance program there will be little confidence in numerical analyses that estimate the failure rates of electronics and the system.


In general, the risks involved in electronics are controlled through design, assembly, test practices, and through the selection and testing of the EEE parts used in the circuits. The risks associated with parts application must include assumptions regarding the performance of the EEE parts under the variety of environmental factors the electronics will encounter.

There is no *a priori* prescription for low-risk electronics. Even a Grade 1 Class “S” parts program can be defeated by improper parts application and stress issues rooted in design or unforeseen vibration and thermal environmental interactions with parts assembled on the board.

Unscreened commercial parts may perform as well as Class “S” parts or they could fail prematurely due to reduced margins not exposed during board- or box-level testing waiting for the right combination of voltage, temperature, mechanical, or operational conditions to fail.

Parts can be used with success if controlled by a top-down assurance program that assures the parts will perform as expected and as intended in the critical applications driving mission risk and safe return of the crew. Assuring parts quality requires a supply chain management approach tied to the top-down assurance program.

The risks associated with the EEE parts are controlled through an assurance program consisting of manufacturing controls, derating criteria, and qualification and screening tests that assure that they will perform as expected under the given mission environment, application, and mission duration.

| | | | |
|---|---|---|----------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 37 of 43 |

The team concluded that any alternative approach for the use of COTS EEE parts in critical applications other than those which have proved successful, such as described in EEE-INST-002, or similar NASA documents, requires a firm basis for substantiation.

To reduce the likelihood that parts failures result in unacceptable mission risk, the NESC recommends the CCP require vehicle providers to: 1) develop and implement a top-down mission assurance program to address EEE parts derating, qualification, traceability, and counterfeit control, and demonstrate how it mitigates the risks associated with EEE parts applications and 2) provide data supporting the effectiveness of the proposed screening approach assuring part failure rates are adequately bounded. Section 8 of this paper provides insight into some of the major characteristics of a parts assurance program.

10.0 Other Deliverables


No unique hardware, software, or data packages, outside those contained in this report, were disseminated to other parties outside this assessment.

11.0 Lessons Learned

No applicable lessons learned were identified for entry into the NASA Lessons Learned Information System.

12.0 Definition of Terms

| | |
|--------------------|--|
| Corrective Actions | Changes to design processes, work instructions, workmanship practices, training, inspections, tests, procedures, specifications, drawings, tools, equipment, facilities, resources, or material that result in preventing, minimizing, or limiting the potential for recurrence of a problem. |
| Finding | A conclusion based on facts established by the investigating authority. |
| Lessons Learned | Knowledge or understanding gained by experience. The experience may be positive, as in a successful test or mission, or negative, as in a mishap or failure. A lesson must be significant in that it has real or assumed impact on operations; valid in that it is factually and technically correct; and applicable in that it identifies a specific design, process, or decision that reduces or limits the potential for failures and mishaps, or reinforces a positive result. |
| Observation | A factor, event, or circumstance identified during the assessment that did not contribute to the problem, but if left uncorrected has the potential to cause a mishap, injury, or increase the severity should a mishap occur. Alternatively, an observation could be a positive acknowledgement of a |


| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 38 of 43 |

Center/Program/Project/Organization's operational structure, tools, and/or support provided.

| | |
|-----------------|---|
| Problem | The subject of the independent technical assessment. |
| Proximate Cause | The event(s) that occurred, including any condition(s) that existed immediately before the undesired outcome, directly resulted in its occurrence and, if eliminated or modified, would have prevented the undesired outcome. |
| Recommendation | An action identified by the NESC to correct a root cause or deficiency identified during the investigation. The recommendations may be used by the responsible Center/Program/Project/Organization in the preparation of a corrective action plan. |
| Root Cause | One of multiple factors (events, conditions, or organizational factors) that contributed to or created the proximate cause and subsequent undesired outcome and, if eliminated or modified, would have prevented the undesired outcome. Typically, multiple root causes contribute to an undesired outcome. |

13.0 Acronyms List


| | |
|-------|--|
| A/D | analog to digital |
| CAD | Computer Aided Design |
| CCF | Common Cause Failure |
| CCP | NASA's Commercial Crew Program |
| COTS | Commercial off the shelf |
| CP | Commercial Partners |
| cPCI | Compact Peripheral Component Interconnect |
| D/C | direct current |
| DPA | destructive physical analysis |
| ECMP | Electronic Component Management Plan |
| EDAC | Error Detection and Correction |
| EEE | Electrical, Electronic and Electromechanical |
| ER | Established Reliability |
| ESD | Electrostatic Discharge |
| FET | Field Effect Transistors |
| FMEA | Failure Modes and Effects Analysis |
| GIDEP | Government-Industry Data Exchange Program |
| GSFC | Goddard Space Flight Center |
| IEC | International Electro-technical Commission |

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 39 of 43 |

| | |
|----------|---|
| IEC-TS | IEC-Technical Standard |
| ISS | International Space Station |
| LOC | Loss Of Crew |
| LOM | Loss Of Mission |
| MIL-HDBK | Military Handbook |
| MIPS | Millions of Instructions Per Second |
| MTSO | Management Technical Support Office |
| NEA | Non-Explosive Actuators |
| NEPP | NASA Electronic Parts and Packaging Program |
| NESC | NASA Engineering and Safety Center |
| PCB | Printed Circuit Board |
| PDA | Percent Defective Allowable |
| PEM | Plastic Encapsulated Microcircuit |
| PIND | Particle Impact Noise Detection |
| PMP | Parts, Materials, and Processes |
| PPAP | Production Part Approval Process |
| PRA | Probabilistic Risk Assessment |
| RDSon | Resistances Drain to Source (when) On |
| RoHS | Restriction of Hazardous Substances |
| SCD | Source Control Drawing |
| TDT | Technical Discipline Team |
| TS | Technical Specification |

14.0 Appendices

- A. Original Request
- B. Data Supporting NEPP Relative Failure Rate Factors

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 40 of 43 |

Appendix A. Original Request


Objective:

Collect additional data to help frame the technical, cost, and schedule risk trades associated with EEE parts selection and specifically the expressed desire of some of the CCDEV2 partners to employ parts of a lower grade than traditionally used in most safety critical NASA applications.

Background:

CCPs CCDEV2 SAAs are actively progressing. Commercial Partners (CPs) are reviewing the CCP draft requirements, which includes the 1130 and 1140 volumes. In 1130, in addition to several performance requirements such as an overall Loss of Crew Probability and Loss of Mission Probability requirement, there are also specific technical requirements associated with Engineering technical stds. On EEE Parts, the CCP engineering teams selected a DoD Std (SMC-S-010 (2009), AFSC Space And Missile Systems Center Standard: Parts, Materials, and Processes (PMP) Technical Requirements For Space and Launch Vehicles (12 Jan 2009)) as the basis for what the CPs need to meet the intent of. The team selected this std with the expressed intent of allowing the partners to trade away from the highest grade parts (Grade 1, Class S, etc.) for lower grade when justified by an analysis which considers circuit criticality as well as mission duration and the program risk tolerance as defined by LOC and LOM. In general, while the CCP EEE parts team considered the ability to trade to a lower part grade a reasonable step, most felt this would be a trade between Space grade and full military grade parts (Class B, JANTX, etc.). Recently, during a round of technical TIMs at least one partner has express an interest in using parts procured from a commercial online distributor (██████) using the industrial grade (due to temperature range limitations) and do little to no upscreen or testing on the component at the piece part-level before installing in the board or assembly. Their rationale to support this approach was that:


1. Extensive testing at the board-and box-level equates to some portion of the testing required to be classified as a higher grade part.
2. Their architecture, which is dual failure tolerance at the system-level as well as internal to the avionics boxes, is robust to failures.
3. The overall increase in failure rates given these lower grade parts, when this 3-string architecture is considered, does not appreciably increase LOC or LOM.
4. The use of commercial parts means a greater part selection with more nimble part lines which generate higher performing parts (higher millions of instructions per second (MIPS), lower RDSon, etc.), which offsets failure rates as performance margin is increased.
5. In addition to performance, their designs can employ newer technologies not available in the Class S Grade 1 versions.
6. The obvious gains in schedule and cost trades.

| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 41 of 43 |

CCP EEE parts teams have heard this approach but have not been provided any formal data. The team's initial reaction is that given our mission durations (15 minutes for launch vehicle and 6 months for Spacecraft) it could be possible that a statistical analysis could support the use of commercial or industrial grade parts with only a minor impact to LOC or LOM. However, overall, the EEE parts team within the CCP are asking for analytical support from the CPs to support their assertions.

Actions:

1. Provide back to the CCP Engineering leadership a benchmark on EEE parts selection criteria from commercial aviation large and small (Boeing Seattle and Cessna or equivalents). It is understood that the mission duration as well as natural and induced environments are different. However, this data point may help program decision-makers frame this risk.
2. Given a generic architecture with dual redundancy across all elements, an assumption that common parts exist in each string, a typical division of LOC/LOM allocation to avionics, can a move from Grade 1/Class S parts to Commercial/Industrial parts with no upscreen really have little effect on overall LOC/LOM? A notional analysis is requested to assess this assertion.
3. Given failure rates collected in Grade 2 upscreens (PIND, X-ray, burn in, etc.) and data from manufacturers and the field centers, can this assessment team recommend an upscreen/testing regime that would improve the analysis in 2 such that the LOC/LOM with commercial grade parts approaches that calculated when Grade 2 (Class B, etc.) parts are used?
 - a. Please provide a primer of parts grades and associated testing of each along with as assessment of what tests provide the greatest value.
4. How does the short mission durations play into the analysis above and does the analysis support a different answer between launch vehicle and spacecraft?
5. How does CCFs play into the results? Given the likelihood of similar strings, and hence similar parts in similar lots across all the legs of redundancy, does common cause dominate the analysis results?

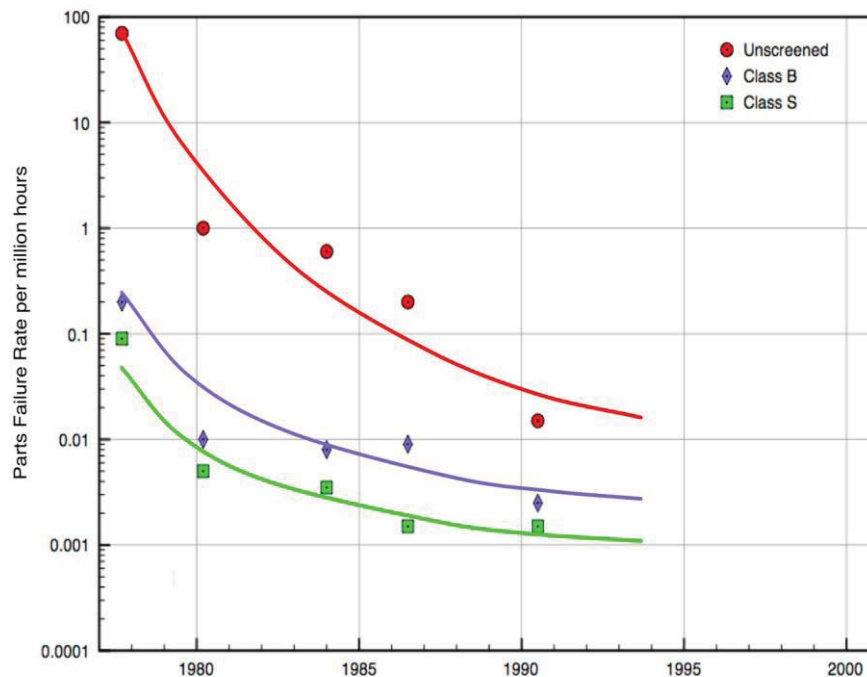
| | | | |
|---|---|---|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP- 12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 42 of 43 |


Appendix B. Data Supporting NEPP Relative Failure Rate Factors

Recent data providing a definitive comparison of Grades 1, 2, 3, and unscreened commercial parts failure rates was not found. There is no doubt parts failure rates have been decreasing and have continued to decrease since the 1990 to 1995 time frame. There is some debate, however, if the lower bounds have been reached due to the advent of computer aided design chip tools which have enabled smaller feature sizes, higher speed operation, along with denser die operating at lower voltages. There is some evidence that the consumer electronics industry's targeted design life of 2 to 5 years have an influence EEE parts wear-out life.

Two data source indicate the relative reliability factors referenced in the white paper's Table 5.0-1 are comparable to data available from the 1990 to 1995 time frame.

Raw failure rate data points from Quality Magazine (Plum, 1990) replotted with approximate trend lines. This source from 1990 shows the failure rate for unscreened commercial parts were more than 10 times higher than Class S Parts. These data also show there is no single deterministic failure rate factor but implies some variability in the relative failure rate factor of 40 for unscreened parts.



| | | | |
|---|---|--|------------------------|
|  | NASA Engineering and Safety Center Technical Assessment Report | Document #: NESC-RP-12-00762 | Version: 1.1 |
| Title: Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program | | | Page #: 43 of 43 |

MIL-HDBK-217 provides parts quality for many different part types. Four common part types are compared in the table below. The parts quality factors approximately support the relative factors referenced by the white paper's Table 5.0-1.

Excerpts from MIL-HDBK-217F 28-Feb-1995 as Relative Factor to Class S:

| Part | Micro Circuit | Diode | Bipolar Transistor | FET Transistor |
|---------------|---------------|----------|--------------------|----------------|
| 217 Paragraph | 5.10 | 6.3, 6.6 | 6.6, 6.7 | 6.4 |
| Class S | 1 | 1, 1 | 1 | 1 |
| Class B | 4 | 3.4 10 | 4 | 3.4 |
| "Lower" | 8 | 7.8 50 | 10 | 7.8 |
| Plastic | | 11.4 100 | | 11.4 |

| REPORT DOCUMENTATION PAGE | | | | | Form Approved OMB No. 0704-0188 | |
|---|-------------|--|-------------------------------|---|---|--|
| <p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p> | | | | | | |
| 1. REPORT DATE (DD-MM-YYYY) 01-04-2012 | | 2. REPORT TYPE Technical Memorandum | | 3. DATES COVERED (From - To) February 2012 - March 2012 | | |
| 4. TITLE AND SUBTITLE Use of Commercial Electrical, Electronic and Electromechanical (EEE) Parts in NASA's Commercial Crew Program (CCP) | | | | 5a. CONTRACT NUMBER | | |
| | | | | 5b. GRANT NUMBER | | |
| | | | | 5c. PROGRAM ELEMENT NUMBER | | |
| 6. AUTHOR(S) Gonzalez, Oscar | | | | 5d. PROJECT NUMBER | | |
| | | | | 5e. TASK NUMBER | | |
| | | | | 5f. WORK UNIT NUMBER 869021.03.04.01.09 | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) NASA Langley Research Center Hampton, VA 23681-2199 | | | | 8. PERFORMING ORGANIZATION REPORT NUMBER L-20134 NESC-RP-12-00762 | | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Aeronautics and Space Administration Washington, DC 20546-0001 | | | | 10. SPONSOR/MONITOR'S ACRONYM(S) NASA | | |
| | | | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) NASA/TM-2012-217558 | | |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT Unclassified - Unlimited Subject Category 38 Quality Assurance and Reliability Availability: NASA CASI (443) 757-5802 | | | | | | |
| 13. SUPPLEMENTARY NOTES | | | | | | |
| 14. ABSTRACT NASA's Commercial Crew and Cargo Program (CCP) is stimulating efforts within the private sector to develop and demonstrate safe, reliable, and cost-effective space transportation capabilities. One initiative involves investigating the use of commercial electronic parts. NASA's CCP asked the NASA Engineering and Safety Center (NESC) to collect data to help frame the technical, cost, and schedule risk trades associated with electrical, electronic and electromechanical (EEE) parts selection and specifically expressed desire of some of the CCP partners to employ EEE parts of a lower grade than traditionally used in most NASA safety-critical applications. This document contains the outcome from the NESC's review and analyses. | | | | | | |
| 15. SUBJECT TERMS Crew and Cargo Program; Commercial off-the-shelf; NASA Engineering and Safety Center; Electrical, electronic and electromechanical parts | | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON | |
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | STI Help Desk (email: help@sti.nasa.gov) | |
| U | U | U | UU | 48 | 19b. TELEPHONE NUMBER (Include area code) (443) 757-5802 | |